CLAIMS:

1. A method for collecting information relating to a communication network, the method comprising:

detecting data conveyed by nodes operating in the communication network in a manner that is transparent to the nodes;

analyzing detected data for identifying the information relating to the communication network and for identifying missing information; and

querying one or more of said nodes for the missing information.

2. The method of Claim 1, wherein the information does not include information relating to network performance.

3. The method of Claim 1 or 2, wherein:

there are received other data relating to the communication network; and

the analyzing detected data analyzes also the other data for identifying the missing information.

4. The method of Claim 1 or 2, wherein the information includes nodal information relating to at least some of the nodes.

5. The method of Claim 4, wherein the nodal information includes operating system information relating to a respective operating system.

6. The method of Claim 5, wherein detecting data conveyed by the nodes includes detecting at least one type of message from a group including DHCP messages and SYN packets.

7. The method of Claim 5 or 6, wherein analyzing includes:

receiving data corresponding to data conveyed by a node;

inspecting received data for characteristics of a known operating system; and

if the data conforms with the characteristics, indicating that the known operating system operates on the node.

8. The method of Claim 4 or 5, wherein the nodal information includes runtime information relating to running processes.

9. The method of Claim 8, wherein information relating to running processes include information relating to network running processes operating on nodes in the communication network.

10. The method of Claim 8, wherein information relating to running processes include information relating to local running processes operating on nodes in the communication network.

11. The method of any one of Claims 4, 5 or 8, wherein the nodal information includes hardware information relating to hardware components associated with the respective nodes.

12. The method of any one of the preceding Claims, wherein the information includes topology information relating to physical topology of the communication network.

13. The method of any one of the preceding Claims, wherein detecting data includes:

capturing data relating to networking traffic;

isolating from captured data networking data that includes information about the communication network; and

conveying the information included in the networking data.

14. The method of any one of the preceding Claims, wherein querying includes:

generating a query message corresponding to the missing information for sending to nodes to be queried;

sending the query message to the nodes to be queried.

15. The method of Claim 14, wherein querying further includes:

receiving at least one response that corresponds to the query message; and

processing the at least one response to retrieve information corresponding to the missing information.

16. The method according to Claim 14 or 15, wherein the query message is an ARP request.

17. The method according to Claim 14 or 15, wherein the query message is an ICMP echo request.

18. The method according to Claim 14 or 15, wherein the query message is a TCP-SYN request.

19. The method of Claim 14, wherein generating is done in accordance with a test policy.

20. The method of Claim 19, wherein the test policy is selected from a group of available test policies.

21. The method of Claim 20, wherein the test policy is selected in accordance with a statistical computation.

22. The method of Claim 14, wherein said missing information relates to at least one running process operating on respective nodes.

23. The method of Claim 14, when used for managing the at least one running process.

24. The method of Claim 14, wherein the data conveyed by nodes includes at least one response that corresponds to the query message.

25. The method of any one of the preceding Claims, when used for providing security control.

26. The method of any one of the preceding Claims, when used for providing management capabilities.

27. A method for collecting information relating to operating systems operating on nodes in a communication network, the method comprising:

receiving data corresponding to a DHCP message conveyed by a node in a manner that is transparent to the node;

inspecting received data for characteristics of a known operating system; and

if the received data conforms with the characteristics, indicating that the known operating system operates on the node.

28. The method of Claim 27, wherein inspecting includes comparing one or more parameters in said received data with the characteristics.

29. The method of Claim 27 or 28, wherein inspecting includes checking if one or more parameters exist in the received data, wherein the one or more parameters are included in the characteristics.

30. The method of any one of Claims 27, 28 or 29, wherein inspecting includes checking content included in one or more parameters of the received data, and the content is compared with the characteristics.

31. A network information collector (**201, 301**) for collecting information relating to a communication network, the system comprising:

a network detector (**203**) for detecting data conveyed by nodes (**103, 104, 106**) operating in the communication network (**101**) in a manner that is transparent to the nodes;

an analyzer (**202**) for analyzing detected data for identifying the information relating to the communication network and for identifying missing information; and

a query engine (**204**) for querying one or more of said nodes for the missing information.

32. The network information collector (**201, 301**) of Claim 31, wherein the information does not include information relating to network performance.

33. The network information collector (**201, 301**) of Claims 31 or 32, further including:

an input device (**801**) for receiving other data relating to the communication network; and

wherein the analyzer (**202**) analyzes also the other data for identifying the missing information.

34. The network information collector (**201, 301**) of Claims 31 or 32, wherein the information includes nodal information relating to at least some of the nodes.

35. The network information collector (**201, 301**) of Claim 34, wherein the nodal information includes operating system information relating to operating systems.

36. The network information collector (**201, 301**) of Claim 35, wherein detecting data conveyed by the nodes includes detecting at least one type of message from a group including DHCP messages and SYN packets.

37. The network information collector (**201, 301**) of Claims 35 or 36, wherein analyzer further includes includes:

an input device (**1501**) for receiving data, the data corresponds to data conveyed by a node;

a data inspector (**1502**) for inspecting received data for characteristics of a known operating system; and

a data marker (**1503**) for indicating that the known operating system operates on the node.

38. The network information collector (**201, 301**) of Claims 34 or 35, wherein the nodal information includes runtime information relating to running processes.

39. The network information collector (**201, 301**) of Claim 38, wherein information relating to running processes include information relating to network running processes operating on nodes in the communication network.

40. The network information collector (**201, 301**) of Claim 38, wherein information relating to running processes include information relating to local running processes operating on nodes in the communication network.

41. The network information collector (**201, 301**) of Claims 34, 35 or 38, wherein the nodal information includes hardware information relating to hardware components associated with the respective nodes.

42. The network information collector (**201, 301**) of any one of Claims 31 to 41, wherein the information includes topology information relating to physical topology of the communication network.

43. The network information collector (**201, 301**) of any one of Claims 31 to 42, wherein the network detector (**203**) includes:

at least one probe (**206**) capturing data relating to networking traffic;

a filter (**601**) for isolating from captured data networking data that includes information about the communication network; and

an output device (**602**) for conveying the information included in the networking data.

44. The network information collector (**201, 301**) of any one of Claims 31 to 43, wherein the query engine (**204**) includes:

a query message generator (**1809**) for generating a query message corresponding to the missing information for sending to nodes to be queried; and

an output device (**1810**) for conveying the query message to the nodes to be queried.

45. The network information collector (**201, 301**) of Claim 44, wherein the query engine (**204**) further includes:

an input device (**1811**) for receiving at least one response that corresponds to the query message; and

a response processor (**1812**) for processing the at least one response to retrieve information corresponding to the missing information.

46. An operating system monitor (**702**) for collecting information relating to operating systems operating on nodes in a communication network, the operating system monitor comprising:

an input device (**1301**) for receiving data, the data corresponds to a DHCP message conveyed by a node in a manner that is transparent to the node;

a DHCP inspector (**1302**) inspecting received data for characteristics of a known operating system; and

a data marker (**1303**) for indicating that the known operating system operates on the node.